

Release Notes

FortiAnalyzer 7.0.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



November 23, 2021

FortiAnalyzer 7.0.2 Release Notes

05-702-752008-20211123

TABLE OF CONTENTS

Change Log	5
FortiAnalyzer 7.0.2 Release	6
Supported models	6
FortiAnalyzer VM subscription license	6
Management extension applications	7
Supported models for MEA	7
Minimum system requirements	7
FortiRecorder	8
Supported models for FortiRecorder	8
Supported cameras	8
Special Notices	9
Fortinet verified publisher docker image	9
Hyperscale firewall mode	10
Modifying the interface status with the CLI	11
Citrix XenServer default limits and upgrade	11
FortiAnalyzer VM upgrade requires more memory	11
Maximum ADOM limits for FortiAnalyzer	12
Port 8443 reserved	12
Hyper-V FortiAnalyzer-VM running on an AMD CPU	12
SSLv3 on FortiAnalyzer-VM64-AWS	12
Upgrade Information	13
Downgrading to previous versions	13
Firmware image checksums	13
FortiAnalyzer VM firmware	13
SNMP MIB files	15
Product Integration and Support	16
FortiAnalyzer version 7.0.2 support	16
Web browsers	17
FortiOS/FortiOS Carrier	17
FortiADC	17
FortiAI	17
FortiAnalyzer	17
FortiAuthenticator	17
FortiCache	18
FortiClient	18
FortiDDoS	18
FortiDeceptor	18
FortiMail	19
FortiManager	19
FortiNAC	19
FortiProxy	19
FortiSandbox	19
FortiSOAR	20

FortiSwitch ATCA	20
FortiWeb	20
Virtualization	20
Feature support	21
Language support	21
Supported models	22
FortiGate models	23
FortiGate special branch models	25
FortiCarrier models	27
FortiADC models	28
FortiAI models	28
FortiAnalyzer models	28
FortiAuthenticator models	29
FortiCache models	30
FortiDDoS models	30
FortiDeceptor models	30
FortiMail models	30
FortiNAC models	31
FortiProxy models	31
FortiSandbox models	31
FortiSOAR models	32
FortiSwitch ATCA models	32
FortiWeb models	32
Resolved Issues	35
Device Manager	35
FortiSOC	35
FortiView	35
Log View	36
Others	36
Reports	37
System Settings	38
Known Issues	39
Event Management	39
FortiSOC	39
FortiView	39
Log View	39
Others	40
Reports	40
System Settings	40
Appendix A - Default and maximum number of ADOMs supported	41
Hardware models	41
Virtual Machines	42
FortiAnalyzer subscription license	42
FortiAnalyzer perpetual license	42

Change Log

Date	Change Description
2021-10-20	Initial release of 7.0.2.
2021-10-22	Updated Appendix A - Default and maximum number of ADOMs supported on page 41.
2021-10-25	Added 624331 to Known Issues on page 39.
2021-10-26	Added notes to Appendix A - Default and maximum number of ADOMs supported on page 41.
2021-11-18	Added FortiGate-80F and FortiGate-200F to FortiGate models on page 23.
2021-11-23	Added FortiGate special branch models on page 25.

FortiAnalyzer 7.0.2 Release

This document provides information about FortiAnalyzer version 7.0.2 build 0180.



The recommended minimum screen resolution for the FortiAnalyzer GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 6](#)
- [FortiAnalyzer VM subscription license on page 6](#)
- [Management extension applications on page 7](#)
- [FortiRecorder on page 8](#)

Supported models

FortiAnalyzer version 7.0.2 supports the following models:

FortiAnalyzer	FAZ-150G, FAZ-200F, FAZ-300F, FAZ-300G, FAZ-400E, FAZ-800F, FAZ-800G, FAZ-1000F, FAZ-2000E, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F, FAZ-3900E
FortiAnalyzer VM	FAZ_DOCKER, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV (including Hyper-V 2016, 2019), FAZ-VM64-KVM, FAZ-VM64-OPC, FAZ-VM64-Xen (for both Citrix and Open Source Xen)

FortiAnalyzer VM subscription license

The FortiAnalyzer VM subscription license supports FortiAnalyzer version 6.4.1 and later. For information about supported firmware, see [FortiAnalyzer VM firmware on page 13](#).

See also [Appendix A - Default and maximum number of ADOMs supported on page 41](#).



You can use the FortiAnalyzer VM subscription license with new FAZ-VM installations. For existing FAZ-VM installations, you can migrate to a FortiAnalyzer VM subscription license, starting with FortiAnalyzer 7.0.1. See the [FortiAnalyzer 7.0.1 VM License Migration Guide](#).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiAnalyzer 7.0.2.



FortiAnalyzer uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiAnalyzer 7.0 Ports Guide](#).

Supported models for MEA

You can use any of the following FortiAnalyzer models as a host for management extension applications:

FortiAnalyzer	FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F, FAZ-3900E
FortiAnalyzer VM	FAZ_DOCKER, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV (including Hyper-V 2016, 2019), FAZ-VM64-KVM, FAZ-VM64-OPC, FAZ-VM64-Xen (for both Citrix and Open Source Xen)

Minimum system requirements

By default FortiAnalyzer VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiAnalyzer 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiAnalyzer has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some MEAs have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiAnalyzer features or multiple, enabled MEAs.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiSOAR	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM • 500 GB disk storage 	<ul style="list-style-type: none"> • 16 vCPU • 64 GB RAM • No change for disk storage

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiAnalyzer plus the minimum system requirements for the MEA.

FortiRecorder

This section identifies what FortiAnalyzer models support the FortiRecorder module and what FortiCamera models are supported.

Supported models for FortiRecorder

Below is a list of the FortiAnalyzer appliances that support the FortiRecorder module.

Platform	Maximum number of cameras
FAZ-300F	6
FAZ-400E	12
FAZ-800F	16
FAZ-1000F	50
FAZ-2000E	40
FAZ-3000F	50
FAZ-3500G	50
FAZ-3700F	60

Supported cameras

The FortiRecorder module supports the following FortiCamera models:

- FCM-CB20
- FCM-FD20
- FCM-FD20B
- FCM-FD40
- FCM-MB40
- FCM-MD20
- FCM-MD40
- FCM-OB30

Special Notices

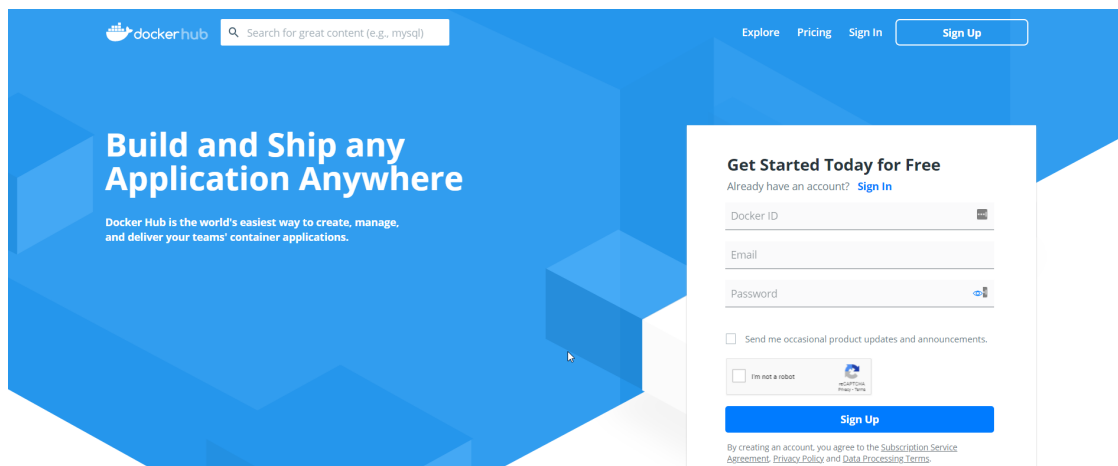
This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 7.0.2.

Fortinet verified publisher docker image

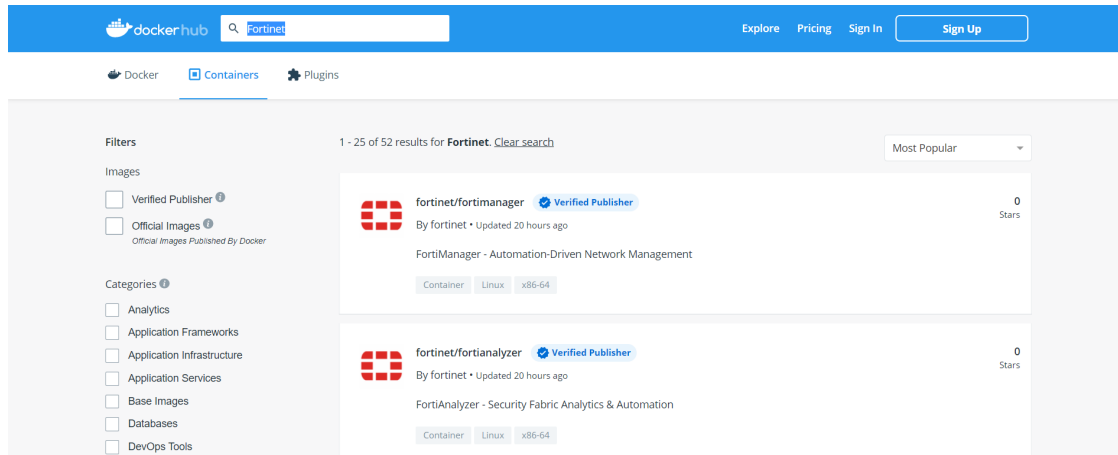
FortiAnalyzer 7.0.1 docker image is available for download from Fortinet's Verified Publisher public repository on dockerhub.

To download the FortiAnalyzer image from dockerhub:

1. Go to dockerhub at <https://hub.docker.com/>.
The dockerhub home page is displayed.

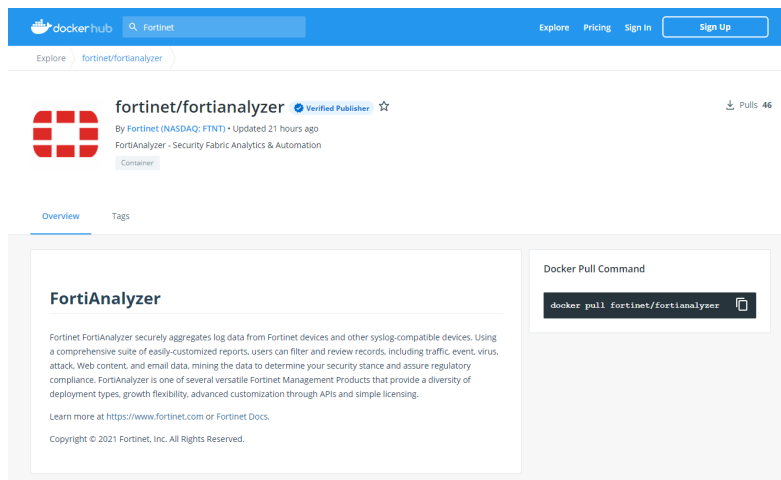


2. In the banner, click *Explore*.
3. In the search box, type *Fortinet*, and press *Enter*.
The *fortinet/fortimanager* and *fortinet/fortianalyzer* options are displayed.



4. Click *fortinet/fortianalyzer*.

The *fortinet/fortianalyzer* page is displayed, and two tabs are available: *Overview* and *Tags*. The *Overview* tab is selected by default.



5. On the *Overview* tab, copy the docker pull command, and use it to download the image.

The CLI command from the *Overview* tab points to the latest available image. Use the *Tags* tab to access different versions when available.

Hyperscale firewall mode

FortiAnalyzer does not support logs from the following models when they have hyperscale firewall mode and netflow enabled:

- FortiGate-1800F
- FortiGate-1801F
- FortiGate-2600F
- FortiGate-2601F
- FortiGate-4200F
- FortiGate-4201F

- FortiGate-4400F
- FortiGate-4401F

FortiAnalyzer only supports logs when the normal firewall mode with standard FortiGate logging are enabled.

Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from `up/down` to `enable/disable`.

For example:

```
config system interface
  edit port2
    set status <enable/disable>
  next
end
```

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FAZ-VM64-XEN image is larger than 128M. Before updating to FortiAnalyzer 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```

2. Confirm the setting is in effect by running `xenstore-ls`.

```
-----
limits = ""
pv-kernel-max-size = "33554432"
pv-ramdisk-max-size = "536,870,912"
boot-time = ""
-----
```

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

FortiAnalyzer VM upgrade requires more memory

When upgrading FortiAnalyzer VM units from FortiAnalyzer 6.2.x to FortiAnalyzer 6.4.0 and later, the upgrade may fail because of memory allocation.

Workaround: Before upgrading FortiAnalyzer VM to FortiAnalyzer 6.4.0 and later, change the memory allocation to 8 GB of RAM.

Maximum ADOM limits for FortiAnalyzer

FortiAnalyzer hardware devices and VMs display a warning when the maximum number of ADOMs is reached or exceeded. The platform does not enforce the limit; however, adding more ADOMs may affect the performance of the unit. For more details, see [Appendix A - Default and maximum number of ADOMs supported on page 41](#).

Port 8443 reserved

Port 8443 is reserved for https-logging from FortiClient EMS for Chromebooks. See also [FortiAnalyzer 7.0 Ports Reference](#) on the Docs Library.

Hyper-V FortiAnalyzer-VM running on an AMD CPU

A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

Upgrade Information

You can upgrade FortiAnalyzer 6.4.0 or later directly to FortiAnalyzer 7.0.2.



For other upgrade paths and details about upgrading your FortiAnalyzer, see *FortiAnalyzer Upgrade Guide*.

This section contains the following topics:

- [Downgrading to previous versions on page 13](#)
- [Firmware image checksums on page 13](#)
- [FortiAnalyzer VM firmware on page 13](#)
- [SNMP MIB files on page 15](#)

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FAZ_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FAZ_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation.

VMware ESX/ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information, see the [FortiAnalyzer Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

Product Integration and Support

This section lists FortiAnalyzer 7.0.2 support of other Fortinet products. It also identifies what FortiAnalyzer features are supported for log devices and what languages FortiAnalyzer GUI and reports support. It also lists which Fortinet models can send logs to FortiAnalyzer.

The section contains the following topics:

- [FortiAnalyzer version 7.0.2 support on page 16](#)
- [Feature support on page 21](#)
- [Language support on page 21](#)
- [Supported models on page 22](#)

FortiAnalyzer version 7.0.2 support

This section identifies FortiAnalyzer version 7.0.2 product integration and support information:

- [Web browsers on page 17](#)
- [FortiOS/FortiOS Carrier on page 17](#)
- [FortiADC on page 17](#)
- [FortiAI on page 17](#)
- [FortiAnalyzer on page 17](#)
- [FortiAuthenticator on page 17](#)
- [FortiCache on page 18](#)
- [FortiClient on page 18](#)
- [FortiDDoS on page 18](#)
- [FortiDeceptor on page 18](#)
- [FortiMail on page 19](#)
- [FortiManager on page 19](#)
- [FortiNAC on page 19](#)
- [FortiProxy on page 19](#)
- [FortiSandbox on page 19](#)
- [FortiSOAR on page 20](#)
- [FortiSwitch ATCA on page 20](#)
- [FortiWeb on page 20](#)
- [Virtualization on page 20](#)



Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

This section lists FortiAnalyzer version 7.0.2 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 93
- Google Chrome version 94

FortiOS/FortiOS Carrier

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiOS/FortiOS Carrier:

- 7.0.0 to 7.0.2
- 6.4.0 to 6.4.7
- 6.2.0 to 6.2.9

FortiADC

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiADC:

- 6.0.2
- 5.4.5

FortiAI

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiAI:

- 1.5.1

FortiAnalyzer

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiAnalyzer:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiAuthenticator:

- 6.0 to 6.2
- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiDDoS

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiDDoS:

- 5.5.0
- 5.4.3
- 5.3.1
- 5.2.0
- 5.1.1
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

FortiDeceptor

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiDeceptor:

- 4.0
- 3.3
- 3.2
- 3.1

FortiMail

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.12
- 5.3.13

FortiManager

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiManager:

- 7.0.0 and later
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiNAC

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiNAC:

- 8.8.0 and later
- 8.7.0 and later
- 8.6.2 and later
- 8.5.4

FortiProxy

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiProxy:

- 1.0 to 1.2

FortiSandbox

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiSandbox:

- 4.0.1
- 3.2.3
- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1

- 2.3.3
- 2.2.2

FortiSOAR

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiSOAR:

- 6.4
- 6.0

FortiSwitch ATCA

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiSwitch ATCA:

- 5.0.0 and later

FortiWeb

This section lists FortiAnalyzer version 7.0.2 product integration and support for FortiWeb:

- 6.3.0 and later
- 6.2.0 to 6.2.4
- 6.1.0 to 6.1.2
- 6.0.0 to 6.0.7
- 5.9.0 to 5.9.1
- 5.8.0 to 5.8.6
- 5.7.0 to 5.7.1
- 5.6.0 to 5.6.1
- 5.5.0 to 5.5.6
- 5.4.1 to 5.4.1

Virtualization

This section lists FortiAnalyzer version 7.0.2 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5, 6.7, and 7.0

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC	✓		✓	
FortiAI	✓	✓	✓	✓
FortiAnalyzer	✓		✓	
FortiAuthenticator	✓			
FortiCache	✓		✓	✓
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓
FortiDeceptor	✓			
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiNAC	✓			
FortiProxy	✓		✓	✓
FortiSandbox	✓		✓	✓
FortiSOAR	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	✓

Language support

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports
English	✓	✓

Language	GUI	Reports
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Russian		✓
Spanish		✓

To change the FortiAnalyzer language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiAnalyzer, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiAnalyzer. For more information, see the *FortiAnalyzer Administration Guide*.

Supported models

This section identifies which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch, FortiWeb, FortiCache, and FortiProxy models and firmware versions can send logs to a FortiAnalyzer appliance running version 7.0.2. Please ensure that the log devices are supported before completing the upgrade.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- [FortiGate models on page 23](#)
- [FortiGate special branch models on page 25](#)
- [FortiCarrier models on page 27](#)
- [FortiADC models on page 28](#)
- [FortiAI models on page 28](#)
- [FortiAnalyzer models on page 28](#)
- [FortiAuthenticator models on page 29](#)
- [FortiCache models on page 30](#)
- [FortiDDoS models on page 30](#)

- [FortiDeceptor models on page 30](#)
- [FortiMail models on page 30](#)
- [FortiNAC models on page 31](#)
- [FortiProxy models on page 31](#)
- [FortiSandbox models on page 31](#)
- [FortiSOAR models on page 32](#)
- [FortiSwitch ATCA models on page 32](#)
- [FortiWeb models on page 32](#)

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-80F, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiWiFi: FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.0

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3301E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-800D-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiGate Hardware Low Encryption: FortiGate-100D-LENC FortiWiFi: FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3301E, FortiGate-3960E, FortiGate-3980E, FortiGate-1800F, FortiGate-1801F, FortiGate-4200F, FortiGate-4201F FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate 7000 Series: FortiGate-7000F FortiGate DC: FortiGate-80C-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3600C-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiGate Hardware Low Encryption: FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC FortiWiFi: FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-80CM, FortiWiFi-81CM, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE FortiGate-VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager FortiGate Rugged: FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiAnalyzer version 7.0.2 supports these models on the identified FortiOS version and build number.

FortiOS 6.4

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-POE, FortiGate-81F-POE	6.4.7	5944
FortiGate-200F	6.4.6	5785
FortiGate-1800F, FortiGate-1800F-DC	6.4.6	5866
FortiGate-1801F, FortiGate-1801F-DC	6.4.6	5868
FortiGate-2600F, FortiGate-2600F-DC	6.4.6	5866
FortiGate-2601F, FortiGate-2601F-DC	6.4.6	5868
FortiGate-3500F	6.4.6	5886
FortiGate-3501F	6.4.6	5876
FortiGate-4200F, FortiGate-4200F-DC	6.4.6	5868
FortiGate-4201F, FortiGate-4201F-DC		
FortiGate-4400F, FortiGate-4400F-DC		
FortiGate-4401F, FortiGate-4401F-DC		
FortiWiFi-80F-2R	1911	5944
FortiWiFi-81F-2R		
FortiWiFi-81F-2R-3G4G-POE		
FortiWiFi-81F-2R-POE		
FortiGate-6000F	6.4.6	1766
FortiGate-7000E, FortiGate-7000F	6.4.6	1766

FortiOS 6.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-POE, FortiGate-81F-POE	6.2.6	7097
FortiGate-200F, FortiGate-201F	6.2.8	7088
FortiGate-1800F, FortiGate-1800F-DC	6.2.7	7104
FortiGate-1801F, FortiGate-1801F-DC		
FortiGate-2600F, FortiGate-2600F-DC	6.2.7	7104
FortiGate-2601F, FortiGate-2601F-DC		
FortiGate-4200F, FortiGate-4200F-DC	6.2.7	7104
FortiGate-4201F, FortiGate-4201F-DC		
FortiGate-4400F, FortiGate-4400F-DC	6.2.7	7105
FortiGate-4401F, FortiGate-4401F-DC	6.2.7	7104

FortiGate Model	FortiOS Version	FortiOS Build
FortiWiFi-80F-2R FortiWiFi-81F-2R	6.2.6	6997
FortiWiFi-81F-2R-3G4G-POE	6.2.6	7099
FortiWiFi-81F-2R-POE	6.2.6	7032
FortiGate-6000F	6.2.6	1158
FortiGate-7000E	6.2.6	1158

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.0
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC	6.2

Model	Firmware Version
FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAI models

Model	Firmware Version
FortiAI: FAI-3500F	1.5
FortiAI-VM: FAI-VM, FAI-KVM	

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E	7.0
FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E	6.4
FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	

Model	Firmware Version
FortiAnalyzer: FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.	6.2
FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	6.0
FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	5.6
FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.	5.4
FortiAnalyzer VM: FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E	6.0 to 6.2
FortiAuthenticator VM: FAC-VM	
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E	5.0 to 5.5
FortiAuthenticator VM: FAC-VM	
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E	4.3
FortiAuthenticator VM: FAC-VM	

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E	4.0, 4.1, 4.2
FortiCache VM: FCH-VM64, FCH-KVM	

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.3, 4.4, 4.5, 4.7

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-1000G, FDC-3000D FortiDeceptor VM: FDC-VM	4.0
FortiDeceptor: FDC-1000F, FDC-3000D FortiDeceptor VM: FDC-VM	3.3
FortiDeceptor: FDC-1000F, FDC-3000D FortiDeceptor VM: FDC-VM	3.2
FortiDeceptor: FDC-1000F, FDC-3000D FortiDeceptor VM: FDC-VM	3.1

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-60D, FML-200D, FML-1000D, FML-3000D, FML-200E, FML-400E, FML-2000E, FML-3000E, FML-3200E, FML-200F, FML-400F, FML-900F	6.4

Model	Firmware Version
FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-60D, FML-200D, FML-1000D, FML-3000D, FML-200E, FML-400E, FML-2000E, FML-3000E, FML-3200E, FML-200F, FML-400F, FML-900F FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	6.2
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E FortiMail Low Encryption: FE-3000C-LENC	5.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B FortiMail Low Encryption: FE-3000C-LENC FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

FortiNAC models

Model	Firmware Version
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.7
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.6
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.5

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E FortiProxy VM: FPX-KVM, FPX-VM64	1.0/1.1

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000F, FSA-2000E, FSA-3000E FortiSandbox-VM: FSA-AWS, FSA-VM	4.0

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox-VM: FSA-AWS, FSA-VM	3.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox-VM: FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.0

FortiSOAR models

Model	Firmware Version
FortiSOAR-VM	6.4
FortiSOAR-VM	6.0

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E	6.3

Model	Firmware Version
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer FortiWeb: FortiWeb-400C, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2
FortiWeb: FortiWeb-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
FortiWeb: FWB-400C, FWB-100D, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0
FortiWeb: FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9
FortiWeb: FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7
FortiWeb: FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E	5.5
FortiWeb VM: FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.4
FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 7.0.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
639479	FortiGate v6.0 with <code>sub-ca</code> certificate may not be able to establish oftp connection with FortiAnalyzer without <code>sub-ca</code> certificate.
687527	CSF cannot be formed when including FortiGate-6000 or FortiGate-7000 series, as blades are not prompted on Device Manager.
724753	Display hidden units is not clickable when there is no unauthorized non-hidden devices present.
731063	FortiAnalyzer supports FortiAuthenticator-300F.

FortiSOC

Bug ID	Description
747193	FortiSoC EMS connector playbook may result in name error.

FortiView

Bug ID	Description
579910	SOC should show AP SSIDs and clients from Event Logs when the Service Profile is in Bridge mode.
640553	FortiView monitor WiFi widget is not showing Bridged SSID information.
678044	FortiAnalyzer may not show rescan icon, and drill-down for rescan may show an empty page.
691570	FortiAnalyzer may not be able to cancel IoC re-scan task.
719441	FortiView may return <code>sql-report dataset</code> query error when <i>Export to Report Chart</i> in FortiClient Software inventory.

Bug ID	Description
722443	Top Destinations on FortiView may not display the correct information.
723799	<i>Policy Name</i> may not show up under <i>FortiView > Traffic > Policy Hits > Policy Column</i> for policies with name information.
724435	SD-WAN performance status widget may be empty if one of the SD-WAN members is down.
726637	FortiAnalyzer should be able to filter on device name and show the device name field properly in the <i>Result</i> column.
731348	FortiView may not apply country filter correctly.
733145	The <i>SD-WAN Events</i> widget may display <i>Invalid params: device: only alphanumeric, '_', '-' and one pair of '[',']' are valid characters.</i>
734359	FortiAnalyzer may return error when applying source IP filter and exporting data to PDF with <i>Top Browsing Users</i> .
735153	IoC incorrectly shows internal host as infected while IPS attack is initiated from outside.
735724	<i>FortiView Monitors</i> page may be showing two <i>Traffic</i> dashboards or <i>VPN</i> dashboards.
748014	FortiView may throw an exception when adding filters for <i>Top Endpoint Vulnerabilities (FortiClient)</i> .

Log View

Bug ID	Description
656507	FortiAnalyzer may lose sorting when clicking the header column in <i>Log Browse</i> .
661094	In <i>Log View</i> , importing logs may fail.
674027	Filtering FortiClient event logs with wildcard <i>UID</i> filter returns no data.
717160	FortiAnalyzer may show duplicated entries when filtering real-time logs in <i>Log View</i> .
726340	<code>oftpd</code> may not work properly if many log requests are received at the same time.
727355	FortiAnalyzer may take very long time on log searches.
745724	Bandwidth data from SD-WAN event logs may not be inserted.

Others

Bug ID	Description
615795	Some IPS packets may be missing on FortiAnalyzer.

Bug ID	Description
621473	FortiSOC is missing in cloud-based VMs.
682539	Local Connector Update Endpoint may fail due to endpoint's record contains unicode characters.
687180	When using the operator <code>>=</code> for "Greater than or Equal to" in FortiAnalyzer CLI, it does not accept the syntax and throws an error.
716576	User with read-only permissions cannot get the list of ADOMs via JSON request.
726012	FortiAnalyzer requires a FortiGuard Indicators of Compromise license in order to see compromised hosts.
726782	The percent of used memory is much higher in 7.0 than 6.4.
729741	An error message may appear on console during upgrade.
730554	FortiAnalyzer HA may use high memory usage.
731070	FortiAnalyzer should add support for FortiNAC v9.1 in <code>supported-platforms</code> .
731319	There may be high memory usage on logfwd with FortiAnalyzer collector.
733792	JSON RPC may fail with code <code>-32603</code> .
735510	<code>sqllogd</code> may cause high memory usage.
744293	Several extra ports are opened when scanning FortiAnalyzer HA cluster's virtual IP.
744918	<code>fortilogd</code> may not write logs for FortiGate-401E-DC.
745025	HMAC given in <code>log-checksum md5-auth</code> option does not match.
746022	There may be multiple <code>siemdbd</code> crashes on <code>redisAppendCommand</code> .
746625	<code>siemagentd</code> may crash.

Reports

Bug ID	Description
677090	Report Filter may not work with devname.
715680	Default chart <i>VPN User Logins</i> may return different values in two reports for the same device or data range.
726688	All predefined report/template/chart/macro/dataset may be missing from newly created ADOM after a reboot.
728923	Log type selector for FortiGate has duplicate traffic log field names due to <i>FortiClient Traffic</i> is changed to <i>Traffic</i> .
734152	Report group filter may not work in FortiProxy ADOM.

Bug ID	Description
734167	Report log field filter drop-down may be missing pick-list in non FortiGate ADOM.
744024	FortiAnalyzer is unable to disable and remove reports from hidden ADOM.
744915	FortiView summary does not match with the sessions shown in the session table.

System Settings

Bug ID	Description
672273	Initial data sync may never finish on Azure or GCP HA cluster unless "diag test app clusterd 97 init-sync done" is run.
710986	An existing log forwarding entry is gone after its status changed from <i>On</i> to <i>Off</i> .
721627	FortiAnalyzer HA cluster always uses VIP for log forwarding to server instead of another interface.
730296	RADIUS authentication using <code>mschap2</code> may not work.
739136	Task monitor shows incorrect user for newly created ADOM.

Known Issues

The following issues have been identified in FortiAnalyzer version 7.0.2. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Event Management

Bug ID	Description
691220	Event handler may not be triggered correctly when there is more than one match.

FortiSOC

Bug ID	Description
717841	IOC events and FortiGate Event Handler events are not being sent to FortiGate from FortiAnalyzer.

FortiView

Bug ID	Description
641596	FortiAnalyzer may show "No Data" in "User Vulnerabilities Summary" widget.
727056	SD-WAN Monitor may show incorrect bandwidth.
741910	Top Cloud Applications may show 0 KB utilization under the Bandwidth column.
744910	<i>Bandwidth</i> should not be used in the FortiView's graphs or tables when they are actually showing <i>bytes received and sent</i> .

Log View

Bug ID	Description
704206	When filtering with "Action" and "Source IP" under Traffic menu, the filter output may be incorrect with the combination of smart action with any other field.

Bug ID	Description
691552	FortiAnalyzer may be missing a double quote in direction log field.

Others

Bug ID	Description
616355	FortiGate may display "SSL error" or "OFTP error" when testing connectivity with FortiAnalyzer.
701753	SIEM database should be trimmed at the same time when quota enforcement occurs.

Reports

Bug ID	Description
653207	FortiAnalyzer may have incorrect dataset queries without considering the 'direction' field.
740220	Log field list for filter may be empty with FortiClient ADOM.

System Settings

Bug ID	Description
624331	<i>System Settings > License Information</i> widget should not display <i>Security Operations/SOC Service</i> for unsupported devices, such as FAZ-200F and FAZ-300F.
653371	CEF log forwarding start time does not match with event time.
669402	FortiAnalyzer may not time out admin a session after many hours.
708958	Changing Timezone on FortiAnalyzer does not take effect on FortiSOC.
734001	FortiAnalyzer HA may randomly fail-over.
742804	TACACS user is not able to browse <i>Log View</i> .
748107	Additional timestamp, <i>tz</i> field, is being added to forwarded logs from FortiAnalyzer.

Appendix A - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiAnalyzer hardware models and virtual machines.

See also the [FortiAnalyzer Data Sheet](#).

Hardware models



For ADOM subscription licenses, FortiAnalyzer enforces the ADOM limits.

For hardware models that do not support the ADOM subscription license, ADOM limits are recommended, but not enforced.

FortiAnalyzer supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FAZ-3000G series, which allows you to use up to a maximum of 1200 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiAnalyzer Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
Desktop models	1		1
300F/300G and 400E Series	25		25
800F/800G and 1000F Series	50		50
2000E Series	250		250
3000F Series	500		500
3000G Series	500	✓	1200
3500F/3500G	500		500
3700F Series	1200		1200
3700G Series	1200	✓	10,000

Virtual Machines



For subscription licenses, FortiAnalyzer enforces the ADOM limits.
For perpetual licenses, ADOM limits are recommended, but not enforced.

FortiAnalyzer subscription license

Five (5) ADOMs are included with FortiAnalyzer VM subscription licenses. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

FortiAnalyzer perpetual license

Recommended maximum number of ADOMs supported:

FortiAnalyzer Platform	Default number of ADOMs
1 GB/Day < License <= 5 GB/Day	10
5 GB/Day < License <= 25 GB/Day	25
25 GB/Day < License <= 100 GB/Day	50
100 GB/Day < License <= 500 GB/Day	250
500 GB/Day < License <= 1000 GB/Day	500
1000 GB/Day < License <= 5000 GB/Day	800
License > 5000 GB/Day	1200



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.